



61 Wildcat Rd
Toronto, ON M3J 2P5
Tel: 1 888 219-2111
www.radiant.net

**Annual 47 CFR § 64.2009(e) CPNI Certification Template
EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 28, 2019

2. Name of company(s) covered by this certification: Radiant Communications Corp

3. Form 499 Filer ID: 832824

4. Name of signatory: Edmund Chislett

5. Title of signatory: President

6. Certification: I, Edmund Chislett, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47CFR § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

A handwritten signature in black ink, appearing to read "Edmund Chislett", written over a horizontal line.

Attachments: Accompanying Statement explaining CPNI procedures

RADIANT COMMUNICATIONS CORP.
STATEMENT OF CPNI OPERATING PROCEDURES

Radiant Communications Corp. (“Radiant”) has implemented policies and procedures that ensure compliance with the rules of the Federal Communications Commission (“FCC”) pertaining to the use, disclosure, and access to customer proprietary network information (“CPNI”), 47 C.F.R. 64.2001 et seq. Below is a summary of such policies and procedures:

(a) Radiant may use, disclose, or access CPNI if it is necessary to the provision of the service to which the information relates. Except as required by law, or as permitted by FCC rules, Radiant will obtain the customers consent prior to using or disclosing CPNI.

(a) Radiant does not use CPNI relating to its U.S. customers to conduct outbound marketing or in connection with its sales and marketing campaigns or for any other reason for which customer approval would be required under 47 C.F.R. § 64.2007(b). Radiant also does not disclose or permit access to CPNI relating to its U.S. customers to affiliates or third parties for marketing purposes.

(b) Radiant has implemented policies and procedures that restrict and prohibit personnel from accessing, using, or sharing customer data without proper authorization. Radiant trains its personnel with regard to these procedures, and all employees have been informed that disciplinary action would result from violating Radiant’s policies and procedures regarding access, use and disclosure of customer data.

(c) Radiant does not provide VoIP or telecommunications services to non-business customers located in the United States. All of Radiant’s U.S. customers have dedicated account representatives and services provided to customers located in the United States are provided pursuant to a contract that addresses Radiant’s use and protection of customer data. Radiant has implemented procedures to authenticate its U.S. customers in accordance with the applicable contract.

(e) Radiant takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Among other measures, Radiant has adopted and implemented internal security procedures and other network security protocols, including, encrypting data.

(d) To the best of its knowledge, Radiant has not had a breach of customers’ CPNI. If Radiant were to reasonably determine that a breach has occurred, Radiant would provide timely notice of such breach to the United State Secret Service, the Federal Bureau of Investigation, and the customer, if permitted, in accordance with 47 C.F.R. § 64.2011 and appropriate records maintained.